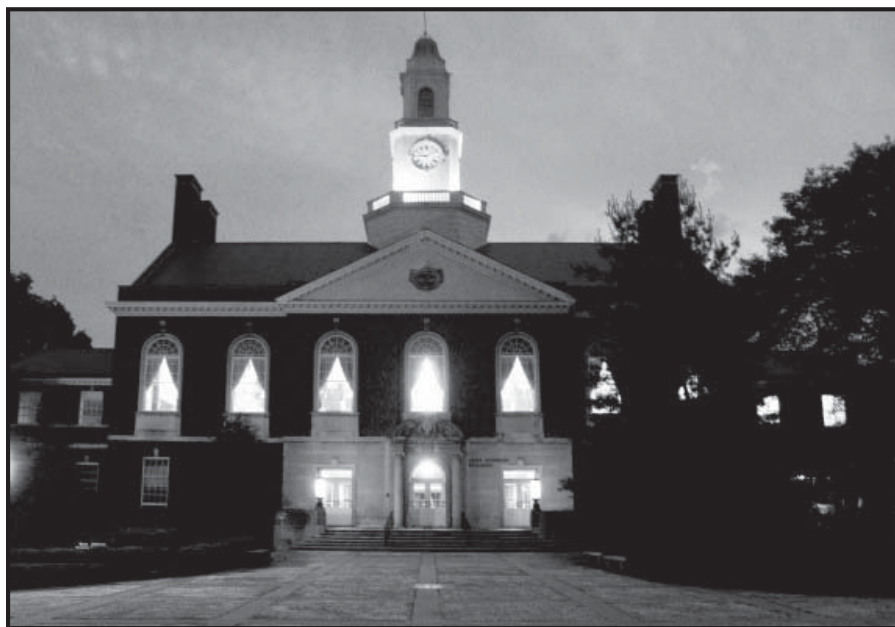


THE WIRE

December 2009

Information Technology news at Eastern

Information Security Issue



Data Security

It depends on you

Managing data can be a daunting task. Trusted data moves across departments as we do the daily tasks of running the University. Making available reliable and accurate data is essential to the operation of the University.

At EKU, computer and network security is a shared responsibility, relying on the awareness and integrity of the campus community. Information Technology staff are continuously trying to anticipate and prevent potential security problems. Our goal is to create a culture in which everyone on campus considers security a part of normal, day-to-day activities.

In this Newsletter, we will talk about how data is stored, how permissions and rights are created and administered, how our drives are setup, the privacy level of each drive, how web crawlers mine data, and other ideas to help you safeguard yourself and the University. Understanding how things work, will help you to be a good steward of the data you touch each day.

Highlights

- Data Security Depends on You
- EKUDirect Login= ECU ID + PIN
- E-Key Username & Password gets you into Email, Network Drives, Blackboard, and more.
- EKUDirect Login is different than E-Key Login
- Keep your ECU ID, PIN and E-Key PRIVATE for your security and the security of the ECU network.
- Rights, authentication and permissions are managed through Active Directory.
- IT Staff will NEVER ask for your username and/or password. Never reply to an email request from ANYONE asking for your E-Key, ID or PIN.
- Be a good steward of data. Data security is contingent on the awareness and integrity of each member of the campus community.

W: Drive at a Glance

STUDENT W: DRIVE

Is that a WEB folder in your drive or are you just that glad to see me? Your W: Drive contains a WEB folder. The files you put in this folder can be seen by everyone.

FACULTY/STAFF W: DRIVE

Protect your private data. The U: Drive is the place to store private files. Never store private information on your W: Drive. W: Drive = Your University web page and can be seen by everyone.



The N and the Q. The P and the U. **Not Sure What They Are?**

The system administrator assigns a letter to a drive.

This is called Drive Mapping. On your computer, the drives are probably mapped like this:

A: floppy disks...if anyone remembers ;

C: hard drive;

D: perhaps a DVD drive, thumb drive or other external device.

Below is a list of the Network Drives and how we use each one.

DRIVES ACCESSIBLE BY FACULTY AND STAFF

N: Drive

Department and college files are stored here. You will have access to your department's files once assigned permission.

PRIVACY LEVEL OF THE N: Drive

Internally viewable by those assigned within your department or college. Not viewable by the general public.

Q: Drive

A campus wide (faculty/staff) public sharing folder. It is used for documents, forms, and applications.

PRIVACY LEVEL OF THE Q: Drive

Internally viewable by those assigned. Not viewable by the general public.

P: Drive

Used for collaborative projects. Users may work on a project with other departments without compromising the security of their N: Drive.

PRIVACY LEVEL OF THE P: Drive

Internally viewable by those assigned. Not viewable to general public.

U: Drive

The employee's personal drive on ECU file servers.

PRIVACY LEVEL OF THE U: Drive

Files on this drive are seen only by the employee.

W: Drive... a little different than the rest:

Faculty, staff and students all have access to the W: Drive but the structure of the student space is a bit different. Faculty and staff: everything you put on the W: Drive can be seen via the web. Students, you have a WEB folder. Here are the details:



PRIVACY LEVEL OF THE W: DRIVE For **STUDENTS...**

The W: Drive is both a private storage drive AND a web—whole world can see it—drive. This dual purpose is accomplished by using a WEB folder located on your W: Drive. Everything you put into this folder is served out to the Internet.

PRIVACY LEVEL OF THE W: DRIVE For **Faculty/Staff...**

The whole world can see what you put on your W: Drive.

The contents of the W: Drive are served out to the web.

Student W:Drive

IT recently changed the structure of the W:Drive for students.

Below is the email that went out a few weeks ago.



What Changed?

Your current W:drive is now PRIVATE storage except the files in the WEB folder. Your web site, and all related graphics, must be moved into this WEB folder for your web site to continue working.

What you need to do:

Move all of your web content to the WEB folder within your W: drive. DO NOT move private files, or files with personal information into the WEB folder. Everything moved to the WEB folder will be accessible via the web and may be crawled by search engines, such as Google. Please be careful not to move files that include your Social Security number or any other sensitive information to the WEB folder.

When did this change occur?

This change went into effect on Friday, November 6, 2009.

For additional information, please visit:

<http://netinfo.eku.edu/faq/student-w-drive-restructuring>

WHERE CAN I find help?

IT WEB site: it.eku.edu

IT HELPDESK: 859.622.3000

IT HOTLINE: 859.622.1411

SMARTCOMPUTING.EKU.EDU



FYI

**Bits & Bytes about
Information Technology**

WHAT IS a Server Farm?

NO CHICKENS or goats; but a lot of cables, computers and software, our Server Farm is the place where programs and data live. Blackboard, Email, ECU Direct, the Network Drives and much more are actually running from the server farm. A server farm is a bunch of networked computers, in many cases, in one location. If one server fails, the remaining server(s) ensure continuous service to the user community.

WHAT IS the Active Directory?

ACTIVE DIRECTORY (AD) is used to store user accounts, assign security policies, and deploy software. AD is the tool through which the system administrators manage your permissions and authentication. Your E-Key tells the AD exactly who you are and what you have permission to see and do.

Best Practice for Data Management

Below are some best practice tips to consider when working with data.

- Keep institutional data on campus.
- Keep data in its original source. For example, if it is on a Network Drive, leave it there, if it is in Banner, leave it there.
- Ask for the least access rights possible to do your job effectively. This protects you as well as the data.
- Know the proper procedures in your area. What is the protocol when an information request is made?
- Consider using a passphrase 12-32 characters instead of a password. For example, theyearIwasborn1984 or myyearofbirthwas1984
- Conduct as little personal business on University equipment as possible.
- Be aware of websites you visit; some sites are notorious for invading your computer with malware and spyware.



**COMPUTER
STORE**

computerstore.eku.edu
859-622-8408

EKU iPhone Cases

Three Different Styles
Compatible with iPhone 3G and 3GS
Only \$15.

Reserve yours today by contacting
the ECU Computerstore at
(859) 622-8408



Web Crawlers

*Helping you find what you want...
and maybe what you don't*

Services like Google use web crawler programs to browse the Internet. These programs provide data for search engines. Web crawlers create copies of pages and the search engine software indexes the pages so that searches will be faster.

You may have had the experience of searching and retrieving a result linking to data that is no longer there. What has happened is that Google—or another search engine—found the data through a crawl program. Depending on your search terms, retained bits of data appear in your search results list even though the site no longer exists.



Even if you remove information from the Internet, some data may still be accessible because it has been mined for a search engine like Google using a web crawler program.



Phishing/Email Scams: Don't Get Caught on the Phishing Hook

Duh duh Duh duh...I think we're going to need a bigger boat.

Have you seen emails that ask you for an account number, login or password? These emails are part of a fraudulent scheme known as "phishing."

Phishers try to wheedle out your private information. These emails can look legitimate.

NEVER GIVE OUT

PRIVATE INFORMATION SUCH AS

**SOCIAL SECURITY NUMBERS,
USERNAMES,**

OR PASSWORDS TO ANYONE!

~ and ~

NEVER RELY

**ON THE APPEARANCE OF AN EMAIL
TO DETERMINE WHETHER IT IS SAFE
TO GIVE OUT YOUR PASSWORD,
BECAUSE IT IS NEVER SAFE
TO GIVE OUT YOUR PASSWORD.**



The sad result of responding to one of these messages is not a pretty picture. Once a phisher has your private information, they can use it to endanger others in our network. If you give out your private information, IT will shut down your account.

What is E-Key?

Students: your E-Key username is the same as the front half of your EKU e-mail address. For example, if your EKU e-mail address is:

mary_smith34@eku.edu

Your E-Key username is:

mary_smith34



Faculty/Staff: your username is your last name followed by your first initial.

For example: **smithm.**

For all, your E-Key password is the same as your email password. Next time you sit at your computer, hit CTRL ALT DEL and type in your E-Key, remember your E-Key is the gateway to your piece of the EKU pie.

What else is tied to E-Key? In addition to your network drive access and email, your E-Key gives you permission to log into Blackboard, Lab Computers, and other programs such as Footprints, SharePoint and AntiSpam.

Never give anyone your E-Key username and password! Guard it with your life. If it gets out, you are vulnerable and all the data you have access to may also be at risk.

What is



EKUDirect

EKUDirect is a Web-based secure link to a wide range of information for employees and students to view and use. Access EKUDirect at www.eku.edu/online. The login is your EKU ID—your Social Security Number will not work—and your initial PIN is your birth date. The first time you login, you will be prompted to immediately change your PIN to a six digit number. This number cannot be your birth date or any part of your SSN. Take care when selecting a PIN—don't make it obvious. Also note that the login and PIN to EKUDirect are different than your E-Key.

**Greetings from the IT Staff
Have a safe and happy winter break.**

The Wire
IT Newsletter
Eastern Kentucky University



Eastern Kentucky University is an Equal Opportunity/Affirmative Action employer and educational institution and does not discriminate on the basis of age, race, color, religion, sex, sexual orientation, disability, national origin or Vietnam era or other veteran status, in the admission to, or participation in, any educational program or activity which it conducts or in any employment policy or practice. Any complaint arising by reason of alleged discrimination should be directed to the Equal Opportunity Office, Eastern Kentucky University, Jones Building, Room 106, Coates CPO 37A, Richmond, Kentucky 40475-3102, 859-622-8020 (V/TDD), or the Director of the Office for Civil Rights, U.S. Department of Education, Philadelphia, PA.

